J. Ryan Mitchell (9362)
Wesley D. Felix (6539)
MITCHELL BARLOW & MANSFIELD, P.C.
Nine Exchange Place, Suite 600
Salt Lake City, Utah 84111
Telephone: (801) 998-8888
Facsimile: (801) 998-8077
Email: rmitchell@mbmlawyers.com
wfelix@mbmlawyers.com

Michael A. Carvin (*pro hac admission pending*)
Ryan J. Watson (*pro hac admission pending*)
JONES DAY
51 Louisiana Avenue, N.W.
Washington, D.C. 20001
Telephone: (202) 879-3939
Facsimile: (202) 626-1700
E-Mail: macarvin@jonesday.com
rwatson@jonesday.com

Attorneys for Plaintiffs

IN THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF UTAH CENTRAL DIVISION

DIGITAL RECOGNITION NETWORK, INC.; VIGILANT SOLUTIONS, INC., Plaintiffs, v. GARY HERBERT, *in his official capacity as Governor of the State of Utah*; SEAN D. REYES, *in his official capacity as Attorney General of the State of Utah*, Defendants.	**PLAINTIFFS' MOTION FOR PRELIMINARY INJUNCTIVE RELIEF AND MEMORANDUM IN SUPPORT** Civil No. 2:14-cv-00099-CW ORAL ARGUMENT REQUESTED

TABLE OF CONTENTS

REQUESTED RELIEF

Pursuant to Federal Rule of Civil Procedure 65, Plaintiffs Digital Recognition Network, Inc. and Vigilant Solutions, Inc. hereby move for a preliminary injunction, without bond, to enjoin the application and enforcement of the Utah Automatic License Plate Reader System Act ("the Act"). *See* 2013 Utah Laws 447 (codified at Utah Code § 41-6a-2001 to § 41-6a-2006, and § 63G-2-305). The Act infringes on Plaintiffs' constitutionally protected speech, in violation of the First and Fourteenth Amendments to the United States Constitution, because it prohibits them, on pain of criminal penalties, from using automatic license plate reader systems to disseminate and collect license-plate data. In support of this motion, Plaintiffs rely on their Complaint, the Memorandum in Support, and the accompanying declarations.

INTRODUCTION

Plaintiff Digital Recognition Network, Inc. ("DRN") uses photographs and image-content analysis techniques to serve the financial services, insurance, and vehicle repossession industries. When DRN and others use such techniques in an effort to locate the alphanumeric content displayed on license plates, this application of the technology is sometimes referred to within the industry as "automatic license plate reader" ("ALPR") technology.[1] DRN's cameras, which are typically mounted on its affiliates' tow trucks, take photographs as the camera-equipped vehicles drive on the public roads. Each photograph is analyzed in order to determine whether it contains a license plate and whether the license-plate number matches the license plate of a vehicle that is sought for recovery by one of DRN's clients, which include automobile lenders and insurance

[1] It is also known within the industry as follows: Automatic Number Plate Recognition (ANPR), Automatic Vehicle Identification (AVI), Car Plate Recognition (CPR), License Plate Recognition (LPR), and Mobile License Plate Recognition (MLPR).

carriers. DRN then disseminates the matching license-plate data to its clients, which use it to locate cars that should be repossessed and to locate cars that have been stolen or fraudulently reported as stolen. Additionally, DRN provides license-plate data to Plaintiff Vigilant Solutions, Inc. ("Vigilant"), which then shares the data with law enforcement agencies for purposes that range from utilizing near real-time alerts for locating missing persons and stolen vehicles to the use of historical license-plate data to solve major crimes such as child abductions. However, the Utah Automatic License Plate Reader System Act, *see* Utah Code § 41-6a-2002 *et seq.* ("the Act"), now prohibits Plaintiffs from using their ALPR systems to disseminate and collect license-plate data in Utah. As a result, Plaintiffs have been forced in Utah to cease engaging in constitutionally protected speech that is vital to their operations. The Act represents a blatant violation of longstanding First Amendment principles and causes Plaintiffs imminent and irreparable injury. Accordingly, the Act must be preliminary enjoined to prevent the ongoing and continuous violation of Plaintiffs' constitutional rights.[2]

Plaintiffs are likely to succeed on the merits of their First Amendment claim. The use of ALPR systems to disseminate and collect information by taking a photograph is constitutionally protected speech. Because the Act's restrictions on such speech are content-based and speaker-based, they are subject to heightened scrutiny, which they cannot survive. In any event, the Act manifestly violates the protections afforded commercial speech even absent such content- and speaker-based restrictions. Specifically, the Act (1) does not further a *substantial* governmental

[2] From a purely technical standpoint, ALPR is not a unique technology, but rather is an application within the field of image-content analysis that utilizes a technique or technology known as Optical Character Recognition ("OCR"). While not accepting or conceding that the Act's definition or description of ALPR is accurate, Plaintiffs will utilize terms such as "automatic license plate readers" and "ALPR" in this memorandum in an effort to avoid confusion.

interest, (2) does not *directly and materially advance* a governmental interest, and (3) *restricts more speech than is necessary* to further the governmental interest at issue. In addition, the numerous gaps and exceptions in the Act further demonstrate that the statute violates the First Amendment.

First, the Utah legislature apparently enacted the Act to advance a purported governmental interest in protecting the "privacy" of publicly-divulged license-plate numbers. The State does not, however, have a substantial interest in preventing persons from viewing or photographing license plates—or from disseminating the information collected when doing so—because license plates contain no sensitive or private information whatsoever. Indeed, the function of license plates is to serve as a government-mandated means of public identification, which makes it irrational for the government to invoke a privacy interest in license-plate data. For these reasons, the State cannot carry its heavy burden to demonstrate that it has a substantial interest in protecting the privacy of license-plate data.

Second, the State cannot demonstrate that the Act directly and materially advances any privacy interest. The only remotely rational governmental interest that could conceivably be invoked here is the interest in preventing the dissemination of license-plate data in circumstances where that data will be *combined with* improperly-obtained personal information derived from another source and then *misused* in a way that creates privacy concerns. Even if this was a substantial governmental interest (which it is not), the Act does not *directly* advance this interest; instead, it is inherently an indirect and attenuated means of furthering the purported privacy interest, because the State is suppressing speech relating to *publicly-displayed license plates* in an effort to prevent misuse of *private data* that might be combined with license-plate

information. Moreover, the Act does not *materially* advance the purported privacy interest, because there is *no evidence* that ALPR systems implicate privacy concerns that are any different from whatever privacy concerns would arise from the disclosure of a single photograph of a license plate or from writing down the license-plate numbers or typing them into a laptop's database.

Third, the speech restrictions in the Act are not adequately tailored because they are more extensive than necessary to serve any purported privacy interest that might be at stake here. In fact, there are numerous obvious alternatives that would impose a lesser burden on speech. Thus, "[i]f protecting privacy is the justification for this law, then the law must be more closely tailored to serve that interest in order to avoid trampling on speech . . . rights." *ACLU v. Alvarez*, 679 F.3d 583, 608 (7th Cir. 2012).

Finally, even if a blanket ban on ALPR use would be constitutionally permissible, the Act's numerous gaps and exceptions fatally undermine the credibility and efficacy of the ALPR restriction's privacy justification. When a statute imposes a selective ban on speech, the government must justify the distinctions and exceptions found in the statute based on its asserted rationale for regulating the speech. In direct contravention of this precedent, however, the Utah legislature enacted a statute that is riddled with inconsistencies and exceptions that arbitrarily permit a wide array of speech that has precisely the same "privacy" implications as speech the statute prohibits. These irrational inconsistencies dramatically undermine the credibility of any claim that the State is concerned about the privacy implications of ALPR usage by entities such as Plaintiffs, or any claim that the statute will substantially cure any "privacy" problems.

Because Plaintiffs are likely to succeed on the merits of their claim, the three other

preliminary-injunction factors are almost invariably satisfied. *See, e.g.*, *id.* at 589 ("in First Amendment cases, 'the likelihood of success on the merits will often be the determinative factor'"). On the irreparable injury factor, "[t]he loss of First Amendment freedoms, for even minimal periods of time, unquestionably constitutes irreparable injury." *Elrod v. Burns*, 427 U.S. 347, 373 (1976) (plurality); *Awad v. Ziriax*, 670 F.3d 1111, 1132 (10th Cir. 2012). Moreover, the remaining factors governing the issuance of a preliminary injunction—the effect of a preliminary injunction on Defendants and the public interest—also tip decisively in favor of Plaintiffs. The State cannot possibly show that it will be harmed by a preliminary injunction, which would simply allow Plaintiffs to engage in additional speech. *Utah Licensed Bev. Ass'n v. Leavitt*, 256 F.3d 1061, 1076 (10th Cir. 2001). And it is well established that there is no public interest to be served in the enforcement of an unconstitutional law. *Awad*, 670 F.3d at 1132 ("'it is always in the public interest to prevent the violation of a party's constitutional rights'").

Accordingly, the Act should be preliminarily enjoined in order to protect Plaintiffs' First Amendment rights.

STATEMENT OF FACTS

A. Plaintiffs' Automatic License Plate Reader Technology

Vigilant develops technology that analyzes photographs and looks for specific content that might be contained within the photograph. At the most basic level, image-content analysis is the extraction of meaningful information from a photograph, and it can be achieved by either a human or by a machine such as a digital camera, mobile phone, computer, processor, or electrical circuit. Image-content analysis tasks can be as simple as reading a bar-coded tag on food packaging or as sophisticated as detecting cancer in an MRI scan. Vigilant executives have

developed image-content analysis techniques for various markets, including techniques for optical character recognition, pattern recognition, and motion detection.

The technique developed by Vigilant involving the use of Optical Character Recognition ("OCR") is the subject of this suit. In one of its applications of image-content analysis, Vigilant utilizes a Digital Signal Processor ("DSP") to convert analog camera output (a photograph) into a digital photograph that can then be analyzed by DSP algorithms to determine if the image contains a pattern that could be representative of a rectangle containing alphanumeric characters (*i.e.,* a possible license plate). Upon location of a possible license plate within an image, the DSP disregards all other aspects of the photograph and performs additional de-skewing, normalization, and character segmentation processes in an effort to improve the chances of successful interpretation or recognition of the printed alphanumeric text contained within the depicted rectangle. The DSP then utilizes OCR algorithms to convert images of text (*i.e.,* alphanumeric characters) printed on the license plate from being only human-readable depictions of text to being both human-readable and computer-readable text.

In short, the technique developed by Vigilant is not capable of doing anything that a human cannot and does not already do—namely, see a license plate, interpret the alphanumeric characters, and make it machine-readable by typing the alphanumeric characters into machine-readable text—but it can do it much faster. Because the subject matter within an image analyzed by the above-referenced technique is a license plate and because the information extracted by such technique is the alphanumeric characters printed on a license plate, these types of applications have sometimes been labeled within the industry as "automatic license plate reader" or "ALPR" systems.

DRN uses image-content analysis technology developed by Vigilant to serve the automobile finance, automobile insurance, and vehicle repossession industries. DRN cameras, which are typically mounted on tow trucks or vehicles owned by repossession companies, automatically photograph everything the camera-equipped vehicle passes during its daily routine of driving on the public streets of its respective city or town looking for vehicles to repossess (for automobile lenders), while simultaneously looking for vehicles that have been reported stolen (for insurance carriers).[3]

Once an ALPR system converts the license-plate image into computer-readable text, software simultaneously cross-checks the alphanumeric characters from the license plate against a database of license plates registered to vehicles that are sought for repossession by lending institutions that DRN serves. DRN then disseminates the matching license-plate data to its clients, which include automobile lenders and insurance companies. DRN earns substantial revenue by selling this license-plate data to its clients. In addition, when there is a match between the captured license-plate data and the database, the software alerts the driver that the vehicle is subject to repossession and prompts the driver to call a dispatch number to verify that the vehicle is still subject to repossession. If the vehicle is verified as still being subject to repossession, then the DRN camera affiliate is authorized to repossess the vehicle.

The ALPR cameras date and time-stamp each digital photograph, as well as recording the GPS coordinates that indicate where the photograph was taken. When this information is captured by a computer in the vehicle, it is uploaded in real time to DRN's data center, where it is stored and processed for use by DRN to aid in recovering vehicles for lending institutions and

[3] The companies that mount DRN's ALPR systems on their vehicles are referred to as DRN's "camera affiliates."

insurance carriers. To date, DRN's ALPR systems have resulted in the successful repossession of over 300,000 vehicles worth more than $2.2 billion and the recovery of almost 4,000 stolen vehicles worth more than $27 million through a partnership with the National Insurance Crime Bureau ("NICB").[4] In addition to serving private clients, DRN also provides its data for free to the National Center for Missing and Exploited Children ("NCMEC") for use in investigating license plates associated with cases involving missing and exploited children. Additionally, DRN provides license-plate data to the NICB to work with law enforcement to locate and recover stolen vehicles and to assist insurance carriers in investigating insurance fraud. Lastly, DRN has a partnership with Vigilant's National Vehicle Location Service, through which DRN's ALPR data is made available to law enforcement agencies—usually at no cost to the agencies. DRN's data thus assists law enforcement in locating missing persons and finding stolen vehicles.

The data that DRN's systems collect—a photograph of the license plate, as well as the date, time, and location—is anonymous data in the sense that it does not contain any personally identifiable information such as the name, address, or phone number of the registered owner. License-plate data thus cannot be linked to a specifically identifiable person unless it is combined with other data, such as vehicle registration records maintained by a state's department of motor vehicles. Access to such motor-vehicle records is, however, strictly regulated by the federal Drivers Privacy Protection Act ("DPPA") and various state laws. The DPPA "establishes a regulatory scheme that restricts the States' ability to disclose a driver's personal information

[4] The number of stolen vehicles recovered in connection with the DRN / NICB partnership does not include vehicles recovered by law enforcement through DRN's partnership with Vigilant's National Vehicle Location Service or the use of in-car ALPR systems by law enforcement. Over the last six years, DRN has provided scan data to law enforcement on more than 700,000 unique stolen vehicles.

without the driver's consent." *Maracich v. Spears*, 133 S. Ct. 2191, 2198 (2013) (internal quotation marks omitted) (citing 18 U.S.C. §§ 2721(a)(1), (a)(2)). In addition, Utah law restricts access to drivers' motor-vehicle records. *See* Utah Code §§ 41-1a-116(1)(a), (3); § 63G-2-202.

B. The Utah Automatic License Plate Reader System Act

The Utah Automatic License Plate Reader System Act provides that, "[e]xcept as provided in Subsection (2), a person or governmental entity may not *use* an automatic license plate reader system." Utah Code § 41-6a-2003(1) (emphasis added). The Act defines an "[a]utomatic license plate reader system" as "a system of one or more mobile or fixed automated high-speed cameras used in combination with computer algorithms to convert an image of a license plate into computer-readable data." § 41-6a-2002(1). Subsection (2), which contains the list of enumerated exceptions, states that "[a]n automatic license plate reader system may be used: (a) by a law enforcement agency for the purpose of protecting public safety, conducting criminal investigations, or ensuring compliance with local, state, and federal laws; (b) by a governmental parking enforcement entity for the purpose of enforcing state and local parking laws; (c) by a parking enforcement entity for regulating the use of a parking facility; (d) for the purpose of controlling access to a secured area; (e) for the purpose of collecting an electronic toll; or (f) for the purpose of enforcing motor carrier laws." § 41-6a-2003(2).

Section 41-6a-2003(1)'s prohibition on the "use" of an ALPR system precludes Plaintiffs from *disseminating or disclosing* license-plate data that is captured by an ALPR system. If this were not the case, the Act would impose no restriction on Plaintiffs' dissemination of captured plate data that it already has in its possession, because the restrictions set forth in § 41-6a-2004(1) and § 41-6a-2004(2) apply only to those persons who obtained captured plate data

pursuant to the statute's enumerated exceptions. *See* § 41-61-2004(1) (imposing restrictions on "[c]aptured plate data obtained for the purposes described in Section 41-6a-2003"); § 41-61-2004(2) (imposing restrictions on "[a] person or governmental entity that is authorized to use an automatic license plate reader system under this part").[5]

In addition, § 41-6a-2003(1)'s ban on the "use" of an ALPR system prevents Plaintiffs from using ALPR systems to *collect* license-plate data. Plaintiffs would therefore violate this provision if they were to use "a system of one or more mobile or fixed automated high-speed cameras" to photograph a license plate and then were to utilize "computer algorithms to convert an image of a license plate into computer-readable data." *See* § 41-6a-2002(1). Importantly, any violation of the Act would subject Plaintiffs to criminal penalties. *See* § 41-6a-2006 ("A person who violates a provision under this part is guilty of a class B misdemeanor.").

Prior to the enactment of the Act in 2013, DRN was collecting ALPR data in Utah and disseminating the data to its clients and partners—including NCMEC, NICB, and Vigilant, which was then sharing the data with law enforcement agencies. *See* Hodnett Decl. ¶ 11. Prior to the Act, DRN sold license-plate data collected by ALPR systems in Utah to clients such as

[5] Section 41-6a-2004(1) restricts the disclosure, use, sharing, and retention of "[c]aptured plate data obtained for the purposes described in Section 41-6a-2003." *Id.*; *see also* § 41-6a-2002(2) (defining "[c]aptured plate data" as "the global positioning system coordinates, date and time, photograph, license plate number, and any other data captured by or derived from an automatic license plate reader system"). For example, "[c]aptured plate data obtained for the purposes described in Section 41-6a-2003" "may not be *used* or *shared* for any purposes other than the purposes described in Section 41-6a-2003" and "may only be *disclosed* . . . in accordance with the disclosure requirements for a protected record under Section 63G-2-202," pursuant to "a disclosure order under Subsection 41-61-2005(2)," or pursuant to a federal or state warrant. § 41-61-2004(1) (emphases added). In addition, § 41-61-2004(2) sets forth additional restrictions on the sharing or sale of "captured plate data" by "[a] person or governmental entity that is *authorized* to use an automatic license plate reader system under this part." *Id.* (emphasis added); *see also* § 41-6a-2003(2) (authorizing ALPR use for purposes that fall within one of the statute's enumerated exceptions).

automobile lenders and insurance companies, thus generating revenue for DRN. *Id.* ¶ 12. In addition, prior to the Act, Vigilant served thirty-three law enforcement agencies in Utah; these law enforcement agencies accessed Vigilant's ALPR data network for the purposes of locating vehicles of interest to law enforcement investigations. Smith Decl. ¶ 9.[6]

As a result of the Act, DRN's Utah camera affiliates have stopped using their ALPR systems, which are the source of DRN's license-plate data. Hodnett Decl. ¶ 14.[7] Moreover, because of the Act, DRN can no longer disseminate or sell license-plate data collected by ALPR systems in Utah. *Id.* Additionally, the Act precludes DRN from selling additional camera kits in Utah to camera affiliates such as repossession companies. *Id.* The Act also prohibits Vigilant from receiving DRN's Utah-based license-plate data and from disseminating this data to law enforcement agencies. *Id.*; Smith Decl. ¶ 12. In short, Plaintiffs' operations in Utah have ceased. Hodnett Decl. ¶ 14; Smith Decl. ¶ 12.

But for the Act, Plaintiffs and their affiliates would resume their collection and dissemination of captured license-plate data using ALPR systems within Utah. Hodnett Decl. ¶ 15; Smith Decl. ¶ 13. But for the Act, DRN and its camera affiliates would collect license-plate data using ALPR systems in Utah, and DRN would then generate revenue by selling this data to clients

[6] Prior to the Act, when law enforcement agencies in Utah made queries against Vigilant's data, the data resulted in investigative leads 39% of the time. Smith Decl. ¶ 10.

[7] Prior to passage of the Act, DRN had sold a total of ten ALPR camera kits to five companies operating in Utah. Hodnett Decl. ¶ 9. Specifically, American Automotive Recovery purchased two kits from DRN at a total cost of $24,575; Network Recovery Systems/Inner Global Recovery Systems purchased three kits at a total cost of $35,275; Repros Recovery purchased three kits at a total cost of $34,313; Recovery First purchased one kit for $8,750; and Swift Towing purchased one kit for $17,000. *Id.* In Utah, American Automotive Recovery began operating DRN's ALPR camera kits in May 2010; Network Recovery Systems/Inner Global Recovery Systems began operating its kits in March 2010; Repros Recovery began operating its kits in January 2011; Recovery First began operating its kit in April 2010; and Swift Towing began operating its kit in February 2012. *Id.* ¶ 10.

such as automobile lenders and insurance companies. Hodnett Decl. ¶ 15. In addition, were it not for the Act, DRN would seek to sell additional camera kits in Utah, thus generating further revenue. *Id.* Finally, but for the Act, Vigilant would receive Utah-based ALPR data from DRN and would disseminate it to law enforcement agencies. Hodnett Decl. ¶ 14; Smith Decl. ¶ 12.

STATEMENT OF THE ELEMENTS

"In order to obtain a preliminary injunction, a movant must establish (1) that it has a substantial likelihood of prevailing on the merits; (2) that it will suffer irreparable injury if the injunction is denied; (3) that the threatened injury to the movant outweighs the injury that the opposing party will suffer under the injunction; and (4) that the injunction would not be adverse to the public interest." *Leavitt*, 256 F.3d at 1065-66.

ARGUMENT

I. PLAINTIFFS ARE LIKELY TO SUCCEED ON THE MERITS.

A. The Act's Restrictions On Plaintiffs' Dissemination And Collection Of License-Plate Information Infringe Speech That Is Protected By The First Amendment.

DRN's and Vigilant's dissemination of the license-plate information collected by ALPR systems is speech within the meaning of the First Amendment, as is DRN's collection and creation of that information by taking a photograph.

1. The dissemination of license-plate data captured by use of an ALPR system is protected commercial speech. In *Sorrell v. IMS Health Inc.*, 131 S. Ct. 2653 (2011), the Court explained that "[a]n individual's right to speak is implicated when information he or she possesses is subjected to 'restraints on the way in which the information might be used' or disseminated." *Id.* at 2665. Indeed, "[i]f the acts of 'disclosing' and 'publishing' information do not constitute speech, it is hard to imagine what does fall within that category." *Bartnicki v. Vopper*, 532 U.S.

514, 526-27 (2001). In *Rubin v. Coors Brewing Co.*, 514 U.S. 476 (1995), the Court invalidated a provision that banned "the disclosure of alcohol content on beer labels" by reasoning that such information "constitutes commercial speech" and that "the free flow of commercial information is 'indispensable . . . in a free enterprise system.'" *Id.* at 478, 481, 488. And in *City of Cincinnati v. Discovery Network, Inc.*, 507 U.S. 410 (1993), the Court struck down a selective ban on commercial newsracks that were used to "distribut[e] . . . commercial publications." *Id.* at 412, 418, 424-30. Thus, dissemination of license-plate data is protected commercial speech.

2. Moreover, as the Court recently reiterated, the First Amendment protects not only the "dissemination of information" for commercial purposes, but also the "creation . . . of information." *Sorrell*, 131 S. Ct. at 2667. This simply reflects the well-established principle that the First Amendment protects the *collection* or gathering of information, particularly where, as here, it is an antecedent step to the dissemination of information and ideas. *See, e.g.*, *Bd. of Educ. v. Pico*, 457 U.S. 853, 866-87 (1982) (plurality); *Richmond Newspapers, Inc. v. Virginia*, 448 U.S. 555, 575-76 (1980) (plurality); *id.* at 583 (Stevens, J., concurring).

The constitutional protections for creating and collecting information apply to speech that is in the form of an image. *See Kaplan v. California*, 413 U.S. 115, 119 (1973). As a result, taking a photograph or otherwise creating an image is firmly protected by the First Amendment. In *United States v. Stevens*, 559 U.S. 460 (2010), the Court concluded that visual depictions such as photographs and electronic images constituted protected expression, and it then struck down a statute prohibiting the commercial creation of certain depictions of animal cruelty. *Id.* at 464-65 & n.1, 468, 482. Similarly, in *Regan v. Time, Inc.*, 468 U.S. 641 (1984), the Court invalidated a statutory provision restricting, among other things, the creation of photographs of U.S. currency.

See id. at 643-44, 648-49. Likewise, lower courts have concluded that the creation, recording, or capture of an image or sound is constitutionally protected, as a corollary of the right to disseminate the resulting image or recording.[8] Of course, absent this constitutional protection, the government could simply ban "photography or note-taking at a public event" as a way of suppressing speech about that event. *Alvarez*, 679 F.3d at 595-96.

In this regard, it is irrelevant that DRN is creating information so it can disseminate it for commercial purposes, rather than to inform the public about political or other matters of public concern. *See, e.g.*, *Sorrell*, 131 S. Ct. at 2665; *Thompson v. W. States Med. Ctr.*, 535 U.S. 357, 366-67 (2002) ("a 'particular consumer's interest in the free flow of commercial information . . . may be as keen, if not keener by far, than his interest in the day's most urgent political debate'"). At most, the fact that it is commercial speech affects the level of scrutiny given to government infringement of that speech (*but see*, pp. 16-19, *infra*); it does not suggest that the First

[8] *See Alvarez*, 679 F.3d at 586-87, 595-96 (enjoining eavesdropping statute as applied to persons who openly make audio recordings of police officers performing official duties in public), *cert. denied*, 133 S. Ct. 651 (2012); *Glik v. Cunniffe*, 655 F.3d 78, 79, 82-83 (1st Cir. 2011) (there is a First Amendment right to film government officials in public); *Smith v. City of Cumming*, 212 F.3d 1332, 1333 (11th Cir. 2000) (plaintiffs had "First Amendment right" to "photograph or videotape police conduct"); *Fordyce v. City of Seattle*, 55 F.3d 436, 439 (9th Cir. 1995) (referring to "First Amendment right to film matters of public interest"); *Dorfman v. Meiszner*, 430 F.2d 558, 560-62 (7th Cir. 1970) (invalidating a rule insofar as it banned photography in certain areas of a federal building and in "the plaza" and areas outside the building); *Cuviello v. City of Oakland*, No. C 06-05517-MHP (EMC), 2007 WL 2349325, at *3, *8 (N.D. Cal. Aug. 15, 2007) (unpublished) (photographing animal abuse is protected speech); *Porat v. Lincoln Towers Cmty. Ass'n*, No. 04-cv-3199-LAP, 2005 WL 646093, at *4 (S.D.N.Y. Mar. 21, 2005) (unpublished) ("communicative photography is well-protected by the First Amendment"); *Demarest v. Athol/Orange Cmty. TV, Inc.*, 188 F. Supp. 2d 82, 93-96 (D. Mass. 2002); *Connell v. Town of Hudson*, 733 F. Supp. 465, 473 (D.N.H. 1990) (First Amendment right to photograph victim of a vehicle collision); *Lambert v. Polk Cnty.*, 723 F. Supp. 128, 133 (S.D. Iowa 1989) (it would violate the First Amendment right "to make . . . videotapes of events" if police were to seize a recording of a fight); *Channel 10, Inc. v. Gunnarson*, 337 F. Supp. 634, 637 (D. Minn. 1972); *Ex parte Thompson*, 414 S.W.3d 872 (Tex. App. 2013), *pet'n for discretionary review granted*, No. PD-1371-13, 2013 Tex. Crim. App. LEXIS 1758 (Nov. 27, 2013) (unpublished).

Amendment fails to protect this speech at all. Indeed, since the media does not enjoy speech or information-gathering protections greater than those of other citizens, *see, e.g.*, *Branzburg v. Hayes*, 408 U.S. 665, 682-84 (1972); *Glick*, 655 F.3d at 83, any suggestion that the creation of photographic images is not protected speech means that the government tomorrow could ban all photography in all public spheres (subject only to rational basis review).

3. Even assuming *arguendo* that collecting photographic information is not itself protected speech, a ban on such collection through use of ALPR systems clearly "burdens" speech by foreclosing the possibility of *disseminating* such information (which is clearly speech). *See Sorrell*, 131 S. Ct. at 2666-67 (concluding that "content- and speaker-based restrictions on the availability and use of prescriber-identifying information" were subject to "heightened scrutiny" because they burdened the speech of pharmaceutical manufacturers who wished to use this information to engage in detailing). Accordingly, the ban on collecting ALPR information is adjudged by the same stringent standards applicable to disseminating such information, particularly since the only articulated or conceivable governmental interest is precluding the purported "privacy" intrusion allegedly created by dissemination.[9]

4. In short, the Act's clear prohibition on any and all "use[s]" of an ALPR system plainly

[9] Moreover, "when speech and nonspeech elements are combined in the same course of conduct," regulation of the "nonspeech element can justify incidental limitations on First Amendment freedoms" only if, *inter alia*, the regulation "furthers an important or substantial governmental interest" and restricts First Amendment rights in a way that "is no greater than is essential." *Arcara v. Cloud Books, Inc.*, 478 U.S. 697, 702-03 (1986) (quotation marks omitted). "First Amendment scrutiny" also applies to statutes that, "although directed at activity with no expressive component, impose a disproportionate burden upon those engaged in protected First Amendment activities." *Id.* at 704; *see Bartnicki*, 532 U.S. at 527. Thus, even if taking a photograph with the intent of disseminating the resulting information constitutes "conduct" rather than speech, the Act's restriction on taking a photograph is subject to First Amendment scrutiny because of the burdens it intentionally imposes on dissemination of information.

outlaws, on pain of *criminal* penalties, Plaintiffs' creation and dissemination of ALPR data. *See* Utah Code §§ 41-6a-2003, 41-6a-2006. The Act thus infringes speech and must be evaluated under the First Amendment standards discussed below.[10]

B. The Act's Regulation Of Speech Is Subject To Stringent Scrutiny.

1. It is axiomatic that the Act imposes a content-based restriction. Its provisions turn on the *content* of what is being photographed and transmitted through ALPR systems—license-plate information is covered, but other content is not. The Legislature has not banned the use of automated high-speed cameras to take all photographs; instead, it has singled out the collection and dissemination of an "image of a license plate" and the resulting "computer-readable data." Utah Code §§ 41-6a-2002(1), 41-6a-2003(1); *see also* § 41-6a-2002(2). And it has singled out this speech because of an (unsubstantiated) fear that captured license-plate data will invade individuals' privacy. Thus, the Legislature justified and crafted its speech restriction based on the content of the speech being regulated.[11]

Moreover, the Act's exceptions demonstrate that it discriminates based on content and the identity of the speaker. The Act expressly authorizes the use of ALPR systems by law enforcement agencies, governmental parking enforcement entities, private parking enforcement entities regulating a parking facility, entities that control access to a secured area, electronic toll collectors, and entities that enforce motor carrier laws. § 41-6a-2003(2). By authorizing the collection and dissemination of license-plate data for "law enforcement," "parking enforcement," etc., but not other purposes, this law constitutes a content-based regulation.

[10] Sections 41-6a-2004(1) and 41-6a-2004(2)—which, as discussed in note 5, *supra*, apply only to persons who obtain license-plate data under the statute's exceptions—also infringe speech.

[11] *Police Dep't of Chicago v. Mosley*, 408 U.S. 92, 95 (1972) ("the First Amendment means that government has no power to restrict expression because of its . . . contents").

In *Regan*, the government ban on printing or photographing a likeness or illustration of U.S. currency was subject to an exception that applied when the photograph was being used for "'philatelic, numismatic, educational, historical, or newsworthy purposes.'" 468 U.S. at 643-44. The Court held that this purpose-based exception meant that the statute "discriminate[d] on the basis of content." *Id.* at 648. Recently, in *Sorrell*, the Court evaluated a law prohibiting *disclosure* of prescriber-identifying information collected by pharmacies for use in marketing, but permitting disclosure for other uses. 131 S. Ct. at 2662-64, 2672. The law also banned *sale* of such information, subject to "exceptions based in large part on the content of a purchaser's speech." *Id.* at 2663. The Court found the statute content-based because, among other things, it "disfavor[ed] marketing, that is, speech with a particular content" and, "disfavor[ed] specific speakers, namely pharmaceutical manufacturers." *Id.*

The Act's broad statutory exceptions also demonstrate that the Act amounts to speaker-based discrimination.[12] Indeed, the Act exempts every (or virtually every) entity that uses ALPR technology except those involved in Plaintiffs' specific business. Additionally, the Act even exempts *technologies* that pose the same (or worse) "privacy" concerns as Plaintiffs' technology, such as technologies that transmit license-plate information in forms other than computer-readable text. *See* pp. 30-35, *infra*. Thus, since the statute authorizes virtually everyone but Plaintiffs and their direct competitors to transmit ALPR or ALPR-like information, it discriminates against certain speakers. *Sorrell*, 131 S. Ct. at 2663.

2. Because the Act's regulation of commercial speech is content- and speaker-based, it is subject to heightened scrutiny. In any event, the Act manifestly violates the protections afforded

[12] *See Citizens United v. FEC*, 558 U.S. 310, 340 (2010) ("restrictions distinguishing among different speakers" are prohibited because they are "often simply a means to control content").

commercial speech against *neutral* regulation under the *Central Hudson* test.

The Court underscored in *Sorrell* that content-based restrictions on commercial speech are subject to heightened scrutiny. 131 S. Ct. at 2664-65. The Court reached this conclusion even on the assumption that the restricted "prescriber-identifying information is a mere commodity." *Id.* at 2667. This conclusion flows naturally from the Court's oft-repeated view that commercial speech is of vital importance. *See, e.g.*, *id.* at 2665; *W. States Med. Ctr.*, 535 U.S. at 366-67. "In the ordinary case it is all but dispositive to conclude that a law is content-based." *Sorrell*, 131 S. Ct. at 2667; *see also Ashcroft v. ACLU*, 542 U.S. 656, 660 (2004). "Under a commercial speech inquiry, it is the State's burden to justify its content-based law as consistent with the First Amendment." *Sorrell*, 131 S. Ct. at 2667. To sustain a content-based burden, "the State must show at least that the statute directly advances a substantial governmental interest and that the measure is drawn to achieve that interest." *Id.* at 2667-68. Finally, "[t]here must be a 'fit between the legislature's ends and the means chosen to accomplish those ends.'" *Id.* at 2668.

Even if heightened scrutiny were inapplicable here, the Court's stringent test for evaluating neutral commercial speech restrictions would apply. To overcome the "presumption that the speaker and the audience, not the Government, should be left to assess the value of accurate and non-misleading information about lawful conduct," the proponent of the commercial-speech restriction must satisfy the test originally set forth in *Central Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n*, 447 U.S. 557 (1980). *Greater New Orleans Broad. Ass'n v. United States*, 527 U.S. 173, 195 (1999) ("*GNOBA*"). Under this test, a court evaluates the "entire regulatory scheme" to determine whether the restriction: (1) furthers a "substantial" governmental interest, (2) "directly and materially advances the asserted governmental interest," and (3) does so in a

way that "is not more extensive than necessary to serve that interest." *Id.* at 183, 188, 192; *see also Leavitt*, 256 F.3d at 1066. The State "bears the burden of identifying a substantial interest and justifying the . . . restriction." *GNOBA*, 527 U.S. at 183; *see Leavitt*, 256 F.3d at 1070-71. "'This burden is not satisfied by mere speculation or conjecture'"; rather, the government "must demonstrate that the harms it recites are real and that its restriction will in fact alleviate them to a material degree.'" *GNOBA*, 527 U.S. at 188; *see Rubin*, 514 U.S. at 487, 490; *Ibanez v. Fla. Dep't*, 512 U.S. 136, 143, 146 (1994). The Act fails these three aspects of *Central Hudson*.

C. The Act Does Not Further A Substantial Governmental Interest.

It appears that the Utah legislature enacted the Act with the hope of advancing a governmental interest in protecting the "privacy" of license-plate data. The Tenth Circuit has, however, warned that courts should be reluctant to embrace "attempts by the government to assert privacy as a substantial state interest." *See U.S. West, Inc. v. FCC*, 182 F.3d 1224, 1234-35 (10th Cir. 1999). Specifically, the Tenth Circuit declared:

> In the context of a speech restriction imposed to protect privacy by keeping certain information confidential, the government must show that the dissemination of the information desired to be kept private would inflict *specific* and *significant* harm on individuals, such as *undue embarrassment or ridicule*, *intimidation or harassment*, or misappropriation of sensitive personal information for the purposes of *assuming another's identity*. . . . A *general level of discomfort* from knowing that people can readily access information about us does not necessarily rise to the level of a substantial state interest under *Central Hudson* for it is not based on an identified harm.

Id. at 1235 (emphases added). Applying these principles, the Tenth Circuit then expressed "doubts" that the government had a substantial interest in preventing the disclosure of "'extremely personal'" and "potentially embarrassing" information such as "when, where, and to whom a customer places [phone] calls." *Id.* at 1228 n.1, 1235, 1236.[13] Needless to say, the

[13] The Tenth Circuit ultimately "assume[d] for the sake of [the] appeal" in *U.S. West* that the

privacy interests in one's private phone calls dwarf any such interest for license-plate numbers.

As discussed in detail below, the State of Utah has utterly failed in the present case to "specifically articulat[e]" a privacy interest such as preventing "ridicule," "undue embarrassment," or the "assuming [of] another's identity." *Id.* at 1235. Indeed, since the Tenth Circuit doubted that preventing disclosure of "'extremely personal'" information about a person's phone calls was a substantial interest, it follows *a fortiori* that preventing disclosure of publicly-available license-plate information cannot constitute a substantial interest. *See id.*

The State does not have a "substantial" privacy interest in preventing persons from photographing or disseminating license-plate data because license plates contain no private information whatsoever. There is no privacy interest in a license plate, which is essentially a "mobile billboard," *see Wooley v. Maynard*, 430 U.S. 705, 715 (1977), that is seen by countless others whenever a vehicle is in public view.[14] To belabor the obvious, a license-plate number is a government-mandated mechanism for *public* identification. Its exclusive (or at least primary) function is to identify the vehicle to which it is attached, so that other private actors (*e.g.,* witnesses to a traffic accident) or public entities (*e.g.,* the police) can ascertain where the vehicle was and when it was there, so as to facilitate the imposition of private and public damages or penalties on the vehicle (or its owner). *See United States v. Ellison*, 462 F.3d 557, 561 (6th Cir. 2006). In short, the purpose and function of license plates is to publicly display information that

(continued…)

interest was substantial, and it then struck down the commercial-speech restriction under the remaining aspects of the *Central Hudson* test. *Id.* at 1236-39.

[14] The State itself recognizes that license plates are, far from being private information, a public pronouncement, which is why it issues "special group license plates" to provide "honor" and "recognition," §§ 41-1a-418(1)(b), (1)(d); *see* § 41-1a-411(2) (regulating personalized license plates so they do not "carry connotations" that are "misleading" or "offensive to good taste").

can be acted on by the public (particularly those who have been injured by the vehicle or its owner). It thus borders on the absurd to suggest that the State has any cognizable, much less substantial, interest in preventing the public from viewing or recording that information, particularly since the State itself mandates the acquisition and public display of that information. *See, e.g.*, Utah Code § 41-1a-401(1) (requiring license plates); § 41-1a-403 (license plates must be "plainly readable"); § 41-1a-404(3)(b)(ii) (license plates must be "clearly legible").

All relevant case law, including binding precedent, confirms the obvious truism that license-plate information is purely public data which cannot be reasonably described as "private" (by even the vehicle owner, much less the government that itself requires the public display). In a case involving a vehicle identification number—which is located *inside* the car but typically viewable from *outside* the car—the Supreme Court held that "it is unreasonable to have an expectation of privacy in an object required by law to be located in a place ordinarily in plain view from the exterior of the automobile." *New York v. Class*, 475 U.S. 106, 114 (1986) ("The exterior of a car, of course, is thrust into the public eye."). Numerous courts have concluded that this reasoning applies to license plates, which are likewise "required by law to be located in a place ordinarily in plain view from the exterior of the automobile."[15]

Dispositively, Tenth Circuit precedent establishes that, "because they are in plain view, no privacy interest exists in license plates." *United States v. Walraven*, 892 F.2d 972, 974 (10th Cir. 1989). Moreover, the Fifth, Sixth, Eighth, Ninth, and Eleventh Circuits have reached the same conclusion.[16] In short, there is no privacy interest in a license plate because "[t]he very purpose

[15] *Id.*; *see United States v. Wilcox*, 415 Fed. App'x 990, 991-92 (11th Cir. 2011) (*per curiam*); *United States v. Diaz-Castaneda*, 494 F.3d 1146, 1151 (9th Cir. 2007); *Ellison*, 462 F.3d at 561.

[16] *Wilcox*, 415 Fed. App'x at 992 ("Wilcox did not have a reasonable expectation of privacy in

of a license plate number . . . is to provide identifying information to law enforcement officials and others." *Ellison*, 462 F.3d at 561.

For essentially the same reason, it cannot be coherently maintained that the photographic *recording* of government-mandated public license plates infringes some privacy interest that concededly is not infringed when the photographer *views* the plate. Since the government commands that the plate be divulged to *all* people in a position to view it, the additional act of recording what everyone can (and must) see entails no invasion of privacy distinct from this universal viewing (even if the photographer distributes the photograph to all members of the public, who can each view the plate without invading the owner's privacy). Nor does Utah think otherwise, since the Act does not prohibit the *photographing* of license plates using low-speed cameras, but only the photographing of license plates using "automated high-speed cameras" in conjunction with "computer algorithms" that "convert [the] image . . . into computer-readable data." §§ 41-6a-2002(1), 41-6a-2003(1).

Additionally, since no privacy interest is infringed when *everyone* sees or records a license plate, no such interest can be infringed if this universally available information is disseminated to others. There is no privacy interest in the underlying data precisely because it is displayed to the entire public, so there cannot rationally be a privacy interest in recording the data, regardless of

(continued…)

the plainly visible license plate"); *Diaz-Castaneda*, 494 F.3d at 1151, 1153 ("people do not have a subjective expectation of privacy in their license plates, and . . . even if they did, this expectation would not be one that society is prepared to recognize as reasonable"); *Ellison*, 462 F.3d at 561 ("a motorist has no reasonable expectation of privacy in the information contained on his plate"); *United States v. Sparks*, 37 Fed. App'x 826, 829 (8th Cir. 2002) ("no person possesses a privacy interest in their license plates"); *Olabisiomotosho v. City of Houston*, 185 F.3d 521, 529 (5th Cir. 1999) ("A motorist has no privacy interest in her license plate number.").

whether it is to be transmitted to a subset of the public that can and does view the license plates directly, without any infringement of privacy.

Also, there is no cognizable "privacy" interest in limiting *one method* by which the public may view data that is publicly available through other means and for which the owner has no cognizable privacy interest to begin with. The Court made this point in a case involving a real and, indeed, "highly significant" privacy interest—*i.e.,* preventing the public disclosure of a rape victim's name. *The Florida Star v. B.J.F.*, 491 U.S. 524, 537, 540-41 (1989) (holding that the government could not prohibit disclosure of the victim's name only in the mass media, but not through other modes of communication).

In short, unlike social security or credit card numbers, license-plate numbers implicate no privacy interest, which is why the government mandates their disclosure, while it restricts the disclosure of social security numbers and credit card numbers. *See* Utah Code §§ 13-44-102(3), 13-44-201(1), 13-45-301(1). Since there is no interest in protecting license-plate numbers from disclosure, the only remotely rational governmental interest that could conceivably be invoked here is the interest in preventing the dissemination of "captured plate data" when (1) that data will be *combined with* personal data derived from another source and (2) *misused* in a way that creates privacy concerns. For example, the ACLU has suggested that "captured plate data" could be integrated with other data and then used to determine the *identity* of a vehicle's *owner*.[17] For a number of reasons, however, this affords no basis for concluding that the Act's speech restrictions further a substantial governmental interest.

[17] *See* ACLU, *You Are Being Tracked: How License Plate Readers Are Being Used To Record Americans' Movements*, at 8-9 (July 2013) (speculating about "[a]busive tracking" of a person's movements, which would necessarily require combining license-plate data with other information that identifies the owner of a vehicle) (hereinafter "ACLU Report").

First, and dispositively, any such argument is effectively a concession that the government has no interest in suppressing information about license-plate data, but only in suppressing *some other* (unidentified) *information* that purportedly may be obtained through some (unidentified) *misuse* of license-plate information. But the government has no substantial interest in prohibiting the use of certain information on the ground that it has valid concerns about *other* (actually private) information, at least absent a compelling showing that the harmless information (license-plate numbers) inevitably creates serious problems in protecting the private data. No such showing, however, has or could be made here.

Moreover, any notion that restricting the use of license-plate data will somehow prevent the misuse of private data is mere conjecture. None of the data that ALPR systems collect—a photograph of the license plate, as well as the date, time, and location—contains personally identifiable information such as the owner's name or address. Moreover, unlike a GPS tracker, this ALPR data cannot be used to continuously *track* a car or individual, given that it is merely a one-time snapshot of a vehicle's location, not a continuous stream of data concerning a person's whereabouts. Nor has the government pointed to a single instance of DRN (or one of its competitors) misusing license-plate data. And, of course, DRN would have *no reason* whatsoever to depart from its profitable business model—*i.e.,* aiding banks and insurance companies in locating cars that are subject to repossession, have been stolen, or have been fraudulently reported as stolen—in order to attempt to identify the vehicle owner by improperly obtaining personally identifiable information and then abusively tracking individuals. (It is absurd to suggest that DRN cares to obtain or disseminate supposedly "private" data such as the identity of a vehicle's owner, given that DRN's clients—such as insurers and lenders—already

have the "private" data that can be obtained through their use of a license-plate number.)

What is more, even if DRN or another entity wished to use license-plate data along with improperly-obtained private data to engage in an effort to establish where a certain individual was at a particular point in time, it could do so only if *the government* released the private information (such as a motorist's driving records) to the entity. But federal and state law severely restrict the release of such information. The DPPA "'establishes a regulatory scheme that restricts the States' ability to disclose a driver's personal information without the driver's consent.'" *Maracich*, 133 S. Ct. at 2198; *see* 18 U.S.C. §§ 2721(a)(1), (a)(2). In addition, Utah law restricts access to drivers' records.[18] Thus, the hypothesized misuse of the ALPR data could only plausibly occur if, despite these statutory protections, the *government* were to release motorists' private information to an entity that then misuses it. This both makes any serious misuse extraordinarily unlikely and dependent upon the unlikely and perhaps improper cooperation of the Government itself. But the Government cannot restrict speech based on such implausible speculation or when the Government itself is responsible for the disclosure. *See GNOBA*, 527 U.S. at 188 (conjecture is insufficient); *Florida Star*, 491 U.S. at 526 (Government could not ban publication of rape victim's name because, *inter alia*, it had disclosed that name).

Finally, misusing ALPR data to identify a vehicle owner's *name* (even if could be done) does not itself implicate privacy concerns. A person's name is hardly private. Privacy is only even arguably relevant if the owner is tracked to various locations using ALPR data and personal information that was improperly obtained. The ACLU has suggested that *law enforcement* entities could and might engage in "tracking." Pets.' Mem. re: Pet. for Writ of Mandamus 3-4,

[18] *See* Utah Code §§ 41-1a-116(1)(a), (3); § 63G-2-202; *Utah Div. of Motor Vehicles – Privacy of Records*, *at* http://dmv.utah.gov/site-menu/privacy-of-records (last visited Feb. 11, 2014).

ACLU v. Cnty. of L.A., No. BS143004 (Cal. Superior Ct. 2014) (citing *United States v. Jones*, 132 S. Ct. 949, 955 (2012) (Sotomayor, J., concurring)). But no one has suggested that commercial users of ALPR like Plaintiffs could or ever would themselves engage in such tracking (and, paradoxically, the Act *exempts* the public law enforcement entities with the means and motive to engage in such tracking, *see* pp. 33-35, *infra*).

In short, even in the ACLU's view, ALPR data arguably implicates "privacy" interests only if it is combined with other government data that was improperly obtained and then abusively used to track the identified vehicle owners. But the Government obviously has no "substantial" interest in a complete ban on certain speech because it hypothesizes that such speech can be combined with other, government-controlled speech and then misused to track owners, particularly when the hypothesized chain of causation requires disclosure by the government itself, is utterly unsupported by any real-world experience, and is facially implausible by all actors other than the law enforcement entities *allowed* to use ALPR.

Nor has Utah even attempted to fill this gaping evidentiary and intuitive void with any findings or evidence suggesting that the highly implausible scenario could occur or has occurred, or even any *articulation* of how public license-plate numbers could be converted into private information. The sum total of the Legislature's explanation of why it wanted to impose a content-based ban on certain speech is that ALPR technology "creates a creepy privacy problem," that technology is "scary," and that ALPR use is analogous to the installation of a tracking chip in every human being's wrist.[19] Needless to say, speech restrictions need to be based on "convincing evidence," *Rubin*, 514 U.S. at 490, not unfounded, ill-defined, barely

[19] Stmt. of Sen. Weiler, Utah State Legislature, Day 39, *video at* http://utahlegislature.granicus.com/MediaPlayer.php?clip_id=3109&meta_id=87212 (remarks at 2:08:42, 2:11:29).

comprehensible, subjective legislative feelings evincing "discomfort." *U.S. West*, 182 F.3d at 1234-35.[20]

D. The Act Does Not Directly And Materially Advance A Privacy Interest.

When the State asserts a privacy interest, it "must show that the dissemination of the information desired to be kept private would inflict specific and significant harm on individuals, such as undue embarrassment or ridicule, intimidation or harassment, or misappropriation of sensitive personal information for the purposes of assuming another's identity." *U.S. West, Inc.*, 182 F.3d at 1235. Utah, however, enacted a law that has *no connection whatsoever* to preventing "ridicule" and the like. License plates are simply a form of public identification. Thus, the State cannot show that the Act advances—let alone *directly and materially* advances—any cognizable interest in protecting people from disclosure of private, embarrassing material.

As noted, the only remotely rational governmental interest that could be invoked here is the interest in preventing the dissemination of "captured plate data" when (1) that data will be *combined with* personal information improperly derived from another source and (2) *misused* in a way that invades privacy. But, by definition, the Act does not *directly* advance this interest. Its restriction on the use of ALPR systems is therefore inherently a very *indirect* means of preventing misuse of *private data* because it protects *other* data—*public license-plate data*—on the theory that this license-plate data has some attenuated connection to that private data.

Nor does the Act *materially* advance the potential interest in preventing misuse of data when improperly-obtained private data such as a vehicle registration record is combined with license-

[20] Assessing whether a purported privacy interest is substantial also involves a "balancing of the benefits and harms of privacy." *U.S. West*, 182 F.3d at 1235. The significant societal benefits of Plaintiffs' ALPR use—including its partnerships with law enforcement, NCMEC, and NCIB—thus confirm that the State has not asserted a substantial privacy interest.

plate data. There is *no evidence* or *finding* that ALPR systems have been misused to improperly access private data or continuously track identified individuals, or that they could plausibly be misused by any non-law enforcement entities, much less companies in Plaintiffs' business. *See Ibanez*, 512 U.S. at 143, 149.[21]

Moreover, as discussed below, *see* pp. 30-35, *infra*, the Act is riddled with so many exceptions that it appears only to encompass one type of actor in the ALPR sphere: Plaintiffs and their direct competitors. *See* § 41-6a-2003(2) (creating a host of exceptions). Thus, even if the collection and dissemination of ALPR data implicated privacy concerns, the Act's myopic focus on Plaintiffs and their competitors—whose use of ALPR systems does not implicate privacy concerns greater than those created by entities falling within the statutory exceptions—is irrational and does not materially advance a privacy interest. *Rubin*, 514 U.S. at 485, 488-89.

The Act also fails to reach a wide variety of other activities that *directly* implicate the privacy concerns that are implausibly and indirectly implicated by use of ALPR data. For instance, the Act does not prohibit a person from sitting outside an abortion clinic and taking photographs of the license plates (or the faces) of all women who enter the clinic. Nor does the Act prohibit a person from engaging in a similar exercise outside an adult movie theater or an Alcoholics Anonymous meeting. Such persons could even post the images of the license plates or people online without violating the Act, thus intruding on privacy to a far greater extent than anything Plaintiffs could do. Because the Act *permits* such collection and dissemination of license-plate information, its ban on Plaintiffs' use of ALPR systems to facilitate vehicle repossession cannot

[21] Moreover, the very "privacy" interest the State is purporting to protect is not even implicated when ALPR data is used to locate a stolen vehicle, because the registered owner is no longer the driver of the vehicle. In addition, a significant number of repossessions occurred on leased vehicles, for which the registered owner is the leasing company as opposed to the lessee.

materially advance any privacy interest.

E. The Act Restricts Speech More Extensively Than Is Necessary To Advance The Government's Purported Privacy Interest.

Under the final step of *Central Hudson*, a speech regulation must not be "'more extensive than is necessary to serve'" the interest at issue. *W. States Med. Ctr.*, 535 U.S. at 367, 371. Thus, the State "must affirmatively establish" a "'fit' between the legislature's ends and the means chosen to accomplish those ends . . . that employs . . . a means narrowly tailored to achieve the desired objective." *Bd. of Trustees v. Fox*, 492 U.S. 469, 480 (1989); *see also Rubin*, 514 U.S. at 490-91. And "if there are numerous and obvious less-burdensome alternatives to the restriction on commercial speech, that is certainly a relevant consideration in determining whether the 'fit' . . . is reasonable." *Discovery Network*, 507 U.S. at 417 n.13; *see also W. States Med. Ctr.*, 535 U.S. at 372; *Revo v. Disciplinary Bd.*, 106 F.3d 929, 935 (10th Cir. 1997).

On its face, Utah's statute is far, far more extensive than necessary to serve the purported interest in preventing the use or dissemination of "captured plate data" in situations where that data will be combined with other improperly-obtained information and then misused. For instance, the Act bans DRN's use of an ALPR system merely to *capture* license-plate data, even if that data is never disseminated to another person. The Act also restricts the dissemination of captured plate data, even when such data is not combined with motorists' personal information. In short, "[i]f protecting privacy is the justification for this law, then the law must be more closely tailored to serve that interest." *Alvarez*, 679 F.3d at 608.

The availability of obvious alternatives that would impose a lesser burden on speech also demonstrates that the Act is not narrowly tailored. One alternative would be for the State to enact a law that contains additional exceptions allowing ALPR use for facilitating repossessions,

for detecting insurance fraud, or for similar legitimate business purposes (or where the recipient of the information already knows the supposedly private information—*i.e.,* the name of the registered owner). These legitimate uses of ALPR data do not implicate the privacy concerns that appear to have animated the Act, so crafting these additional exceptions would permit additional speech without hampering the Act's privacy objectives.

Another alternative would be for the State simply to rely on the DPPA and other similar laws that strictly regulate disclosure of motorists' *personal* information. The DPPA "provides that, unless one of its exceptions applies, a state DMV 'shall not knowingly disclose or otherwise make available' 'personal information' and 'highly restricted personal information.'" *Maracich*, 133 S. Ct. at 2198. Utah law also restricts access to drivers' motor-vehicle records. Utah Code §§ 41-1a-116(1)(a), (3); § 63G-2-202. There is no evidence that these existing laws have failed adequately to protect motorists' data.[22]

F. Even If A Blanket Ban On ALPR Use Would Directly And Materially Advance A Substantial Interest, The Act's Numerous Exceptions And Inconsistencies Fatally Undermine The Credibility Of The State's Purported Privacy Interest.

A selective speech ban must justify the *distinctions* drawn by the government; it does not suffice to hypothesize a mythical, *neutral* speech ban and advance interests relevant to such a straightforward condemnation of speech. This is because exceptions and inconsistencies are often dispositive evidence that the speech is not sufficiently harmful to justify regulation, and that the regulation does not directly advance the government's interest, because it is unlikely to "cure" the relevant "problem" since the "harmful" message may be delivered through other means. *Rubin*, 514 U.S. at 488-89; *see GNOBA*, 527 U.S. at 193; *City of Ladue v. Gilleo*, 512

[22] *See Pac. Frontier v. Pleasant Grove City*, 414 F.3d 1221, 1232-33 (10th Cir. 2005) (holding that a speech restriction failed *Central Hudson* partly because existing laws were adequate).

U.S. 43, 52 (1994); *Discovery Network*, 507 U.S. at 426-28. Moreover, allowing speech by certain speakers but not others constitutes forbidden speaker-based discrimination. *Citizens United*, 130 S. Ct. at 898-99; *GNOBA*, 527 U.S. at 194. In short, if the government imposes a selective speech ban, it must explain why the distinctions among speakers advance its purported interest—*i.e.,* why such speech becomes harmful only when uttered by the targeted speakers.

In *Rubin*, a ban on disclosing beer's alcohol content on *labels* could not "materially advance" the substantial interest in "preventing brewers from competing on the basis of alcohol strength" because the government did not completely ban such disclosures in *advertising*. 514 U.S. at 485, 488. Similarly, a ban on casino advertising in *GNOBA* was invalid because certain speakers were allowed to so advertise, and "select[ing] among speakers conveying virtually identical messages" is impermissible. 527 U.S. at 194. In *Sorrell*, a law banning pharmaceutical manufacturers from using prescriber-identifying information for marketing did "not advance the State's asserted interest in physician confidentiality" because the law "permit[ted] extensive use of [this] information" by other speakers and for other purposes. 131 S. Ct. at 2669.[23] Such exceptions doom even restrictions on speech that *directly* invade *real* privacy interests: In *Florida Star*, the government could not justify its "highly significant" interest in preserving a rape victim's privacy because it had banned disclosure of a victim's name only in mass media, but not in other modes of communication. 491 U.S. at 537, 540-41 ("When a State attempts the extraordinary measure of punishing truthful publication in the name of privacy, it must . . .

[23] In *Discovery Network*, the city had "admittedly legitimate interests" relating to "safety and esthetics" that might have justified banning *all* newsracks from sidewalks, but these interests could not justify a "selective ban" on only *commercial* newsracks. 507 U.S. at 418, 424-30. Similarly, in *Leavitt*, the Tenth Circuit invalidated Utah's restrictions on commercial advertisements for liquor because the statutory provisions at issue drew "irrational distinctions among different types of alcohol." 256 F.3d at 1074, 1075; *Revo*, 106 F.3d at 934.

apply[ ] its prohibition evenhandedly, to the smalltime disseminator as well as the media giant.").

In the present case, the Act contains gaps and exceptions that irrationally permit a wide array of speech that has the same privacy implications as speech the statute prohibits, thus demonstrating that the State cannot possibly have a substantial interest or concern about the privacy implications of Plaintiffs' ALPR usage. Additionally, this "select[ing] among speakers conveying . . . identical messages" refutes any attempt to show that the Act directly and materially advances a privacy interest. *GNOBA*, 527 U.S. at 194.

The Act's irrational coverage gaps demonstrate that Utah has no "substantial" interest in precluding license plate photography and that the Act cannot directly advance any such interest. The Act restricts the "use" only of an "automatic license plate reader system," § 41-6a-2003(1), which is "a system of one or more mobile or fixed automated high-speed cameras used in combination with computer algorithms to convert an image . . . into computer-readable data," § 41-6a-2002(1). Thus, the Act in no way restricts the use of low-speed cameras to photograph license plates. This shows that photographing vehicle owners in "embarrassing" situations does not, in the State's mind, raise substantial privacy concerns. Prohibiting one form of photography (high-speed photography) is not rational, because there is no empirical or logical basis for concluding that the banned speech infringes privacy to a greater degree than the authorized speech. For example, the Act would permit a person to stand outside an abortion clinic with an iPhone, capturing license-plate images and posting them to a website offering searchable license-plate data. Yet, the *permitted* activity raises more serious privacy concerns than Plaintiffs' collection and dissemination of the same data using ALPR systems for repossession purposes.

Similarly, the Act applies only when an automated high-speed camera is used in conjunction

with *computer algorithms* that convert a license-plate image into computer-readable text. § 41-6a-2002(1). But the Act does not, for example, apply to a person who observes license plates and converts the observed license-plate data into alphanumeric text either by writing down the license-plate numbers or typing them into a database on a laptop—even though this would have the *same effect* on privacy as the use of a high-speed camera and algorithms. There is no rational basis for singling out algorithms—and such a narrow prohibition cannot advance Utah's "interest" in precluding dissemination of license-plate data implicating privacy.

Moreover, the Act's gaps demonstrate that the Legislature did not craft the Act with the goal of eliminating *efficient* gathering or dissemination of license-plate data. Indeed, the Act would permit Google or a government property appraiser to send a team of cars to Utah with high-speed cameras mounted on their roofs, so long as Google or the tax appraiser retained the images in their original format instead of converting them into text.[24] In any event, as noted, targeting speech because it efficiently reaches a large audience is invalid. *Florida Star*, 491 U.S. at 540.

The Act's gaps and exceptions also demonstrate that the law is an arbitrary *speaker-based* restriction. The Act creates six express exceptions that authorize the use of ALPR systems by a host of entities. § 41-6a-2003(2). Simply put, the Act allows *all* ALPR entities other than Plaintiffs (or their direct competitors) to use ALPR systems. This is impermissible. *See Citizens United*, 558 U.S. at 340. Moreover, because the Act applies only to Plaintiffs and their competitors, the Act cannot possibly solve whatever privacy problem it is designed to address. Worse still, it is utterly irrational for the Act to target Plaintiffs, because the entities that fall within the exceptions all pose *greater* or at least equal privacy concerns.

[24] *See* Exh. A. A governmental website includes photographs of residences and license plates, personal data, and property values. This poses a far greater "privacy" intrusion than ALPR data.

Most significantly, the Act authorizes ALPR use for law enforcement purposes, even though law enforcement entities (1) are uniquely able to use license-plate data to identify vehicle owners, (2) can "track" those owners, and (3) according to the ACLU, have a very plausible incentive to do so. Because law enforcement entities have access to vast information, the ACLU believes they are especially likely to use a person's license plate to tie him to a crime in a way that trenches substantially on privacy interests. This is why the ACLU's principal concerns have focused on potential *law-enforcement* misuse of ALPR data. *See* ACLU Report, at 12-27. The fact that the Act permits ALPR use by the entities most likely to use license-plate data to invade "privacy," but forbids "identical" speech by Plaintiffs, who are far less likely to do so, is a textbook irrational distinction that dooms a speech restriction. *See Rubin*, 514 U.S. at 485, 488.

Perhaps most irrationally, the Act simultaneously permits police to use ALPR systems to identify stolen cars, but precludes DRN from using such systems to identify cars that, although not stolen by force, are being unlawfully possessed by those who are delinquent on their car payments. This is irrational, because unlike using license-plate data for facilitating vehicle repossession, which does not require identifying the owner, using license-plate data for law enforcement necessarily has as its goal the identification of the owner.

Most specifically, since the Act contains a law enforcement exception, it must, at a minimum, be unconstitutional for the Act (1) to prohibit DRN from sharing ALPR data with Vigilant, NCMEC, and NICB and (2) to prohibit Vigilant, NCMEC, and NICB from sharing that data *with law enforcement*. Vigilant wants to share license-plate data with law enforcement, and it is arbitrary for the Act to preclude it from doing so while simultaneously authorizing law

enforcement agencies to use ALPR systems.[25]

More generally, singling out Plaintiffs (and their competitors) as the only commercial actors who cannot use ALPR is facially unreasonable and fatally undermines both the validity of the State's interest and the ability of the Act to materially advance that interest. It is irrational for the Act to treat Plaintiffs as less trustworthy custodians of ALPR data than the private entities that fall within the statute's exceptions. It makes no sense to authorize private entities to use ALPRs to prevent people from evading a *parking fee or parking regulation*, but bar Plaintiffs' use of ALPRs to facilitate repossession of vehicles when people have failed to make *car payments or have made fraudulent insurance claims*. Surely the State has no interest in helping individuals who are not making car payments cheat their banks out of money that they are owed.

Moreover, there is no evidence that Plaintiffs have ever inappropriately combined license-plate data with improperly-obtained private data to determine where particular individuals were at specific times. And, as noted, Plaintiffs would have no *reason* to misuse ALPR data by combining it with improperly-obtained personal data, because they use ALPR systems only for profit-motivated activities and assisting law enforcement. In the end, if there is no privacy intrusion when parking-enforcement entities collect and disseminate ALPR data to facilitate parking fee collection, there can be no cognizable privacy intrusion when Plaintiffs do so for purposes like facilitating repossessions.

II. THE ACT IRREPARABLY HARMS PLAINTIFFS BY BANNING THEIR USE OF ALPR SYSTEMS TO DISSEMINATE AND COLLECT INFORMATION.

Prior to the Act, DRN was utilizing ALPR systems in Utah. DRN was then disseminating

[25] It is also arbitrary that the Act bans Plaintiffs' ALPR use but permits a bank to send teams to ride around parking lots using low-speed cameras or their eyes, type license-plate numbers into a laptop's database of vehicles that need to be repossessed, and notify the bank of any hits.

license-plate data to its clients and partners—including Vigilant, which in turn was making the data available to law enforcement. The Act has forced Plaintiffs to shutter their operations in Utah. But for the Act, Plaintiffs would resume their constitutionally protected collection and dissemination of license-plate information within Utah. The Act thus irreparably harms them by preventing them from engaging in such speech. The analysis of irreparable harm and the other preliminary-injunction factors turns on the strength of the First Amendment claim,[26] because "[t]he loss of First Amendment freedoms, for even minimal periods of time, unquestionably constitutes irreparable injury." *Elrod*, 427 U.S. at 373 (plurality); *see Awad*, 670 F.3d at 1131; *Leavitt*, 256 F.3d at 1076. Thus, any delay in Plaintiffs' ability to speak is an irreparable infringement on their First Amendment rights that cannot be compensated with money damages.

III. AN INJUNCTION WILL NOT HARM DEFENDANTS OR THE PUBLIC.

Defendants cannot point to any harm to themselves or the public that would result from a preliminary injunction. In cases where a First Amendment claim is likely to succeed, courts routinely hold that the public interest and balance-of-the-equities factors weigh in favor of a preliminary injunction.[27] Moreover, even if this Court were to issue a preliminary injunction but later conclude that Plaintiffs' claim fails on the merits, neither Defendants nor the public would suffer any actual harm. Neither the State nor the public has any conceivable interest in enforcing an unconstitutional law that could outweigh Plaintiffs' interests in conducting their businesses in

[26] *Alvarez*, 679 F.3d at 589 ("in First Amendment cases, 'the likelihood of success on the merits will often be the determinative factor'"); *Kirkeby v. Furness*, 52 F.3d 772, 775 (8th Cir. 1995).

[27] *See Awad*, 670 F.3d at 1132 ("'it is always in the public interest to prevent the violation of a party's constitutional rights'"); *Homans v. City of Albuquerque*, 264 F.3d 1240, 1244 (10th Cir. 2001) (*per curiam*); *Leavitt*, 256 F.3d at 1076 (balance of harms favored plaintiff); *Johnson v. Minneapolis Park & Rec. Bd.*, 729 F.3d 1094, 1102 (8th Cir. 2013); *Alvarez*, 679 F.3d at 589-90; *ACLU v. Ashcroft*, 322 F.3d 240, 247, 250-51 & n.11 (3d Cir. 2003), *aff'd*, 542 U.S. 656 (2004).

accordance with their First Amendment rights. *See* note 27, *supra*. In fact, the law's prohibition on Plaintiffs' speech *harms* the public interest, because the "'disclosure of truthful, relevant information is more likely to make a positive contribution to decisionmaking than is concealment of such information.'" *Ibanez*, 512 U.S. at 142. Moreover, DRN sends license-plate data to Vigilant, which shares it with law enforcement for free—but the Act now bans this information sharing, thus hampering law enforcement efforts to locate missing persons and stolen vehicles. In short, Defendants cannot credibly claim that they or the public would be harmed simply by the additional speech that would result if Plaintiffs were allowed to re-start their operations in Utah.

CONCLUSION

Plaintiffs respectfully request that the Court hold argument and preliminarily enjoin the Act.

Dated: February 13, 2014

Respectfully submitted,

/s/ J. Ryan Mitchell
J. Ryan Mitchell
Wesley D. Felix
Mitchell Barlow & Mansfield, P.C.
Nine Exchange Place, Suite 600
Salt Lake City, Utah 84111
Telephone: (801) 998-8888
Facsimile: (801) 998-8077
Email: rmitchell@mbmlawyers.com

Michael A. Carvin*
Ryan J. Watson*
JONES DAY
51 Louisiana Avenue, N.W.
Washington, D.C. 20001
Telephone: (202) 879-3939
Facsimile: (202) 626-1700
macarvin@jonesday.com
Attorneys for Plaintiffs
**Applications for admission pro hac vice pending*

CERTIFICATE OF SERVICE

I hereby certify that on February 13, 2014, a true and correct copy of the foregoing will be served on the following party via hand delivery, consistent with both Fed. R. Civ. P. 4(e)(2)(A) and 4(j)(2):

Gary Herbert, Governor of the State of Utah
Utah State Capitol Complex
350 North State Street, Suite 200
Salt Lake City, Utah 84114-2220

In addition, I hereby certify that on February 13, 2014, a true and correct copy of the foregoing was served on the following party via certified mail at the following address:

Gary Herbert, Governor of the State of Utah
Utah State Capitol Complex
350 North State Street, Suite 200
PO Box 142220
Salt Lake City, Utah 84114-2220

In addition, I hereby certify that on February 13, 2014, a true and correct copy of the foregoing will be served on Defendant Sean D. Reyes via hand delivery, consistent with Fed. R. Civ. P. 4(e)(2)(A), at the following address:

Sean D. Reyes, Attorney General of the State of Utah
Office of the Attorney General
Utah State Capitol Complex
350 North State Street Suite 230
Salt Lake City, Utah 84114-2320

In addition, I hereby certify that on February 13, 2014, a true and correct copy of the foregoing was served on Defendant Sean D. Reyes via certified mail, consistent with Fed. R. Civ. P. 5.1(a)(2), at the following address:

Sean D. Reyes, Attorney General of the State of Utah
Office of the Attorney General
Utah State Capitol Complex

350 North State Street Suite 230
Salt Lake City, Utah 84114-2320

_/s/_J. Ryan Mitchell_____
J. Ryan Mitchell
Mitchell, Barlow & Mansfield P.C.
Nine Exchange Place, Suite 600
Salt Lake City, Utah 84111
Telephone: (801) 998-8888
Email: rmitchell@mbmlawyers.com